The Barracuda Web Application Firewall Ensures FISMA Compliance

White Paper

RELEASE 1

Barracuda Web Application Firewalls protect networks against unauthorized access, data leakage, site defacement, and other malicious attacks by hackers that compromise both the privacy and integrity of vital data. By installing a Barracuda Web Application Firewall, U.S. federal agencies and contractors can protect their web applications and satisfy key Federal Information Security Management Act (FISMA) compliance controls in one easy step.

Federal Information Security Management Act

Cyber threats to federal information systems have been identified as one of the most serious national security challenges faced by the nation. Cyber exploitation activity has grown more sophisticated, more targeted, and more serious. These threats can be unintentional and intentional, targeted or non-targeted, and can come from a variety of sources, such as foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, and disgruntled employees working within an organization.[1]

In response to this increasing threat to federal information systems, FISMA was enacted under the E-Government Act of 2002 to ensure the protection and defense of U.S. government information systems, assets, and operations. FISMA directs the National Institute of Standards and Technology (NIST) to develop and issue publications to assist agencies with the operational framework and guidelines commensurate with the latest threat landscape.

NIST 800-53 Security Control Classes

NIST Special Publication 800-53 defines the minimum IT security controls for compliance. Publication 800-37 provides a guide for applying a six-step risk-based approach to the accreditation process, the second of which involves selecting the appropriate subset of security controls from NIST Special Publication 800-53.

SANS 20 Critical Security Controls (20CSC)

Due to the large number of control classes, FISMA compliance metrics and reporting can be daunting, especially for large federal organizations. The vast array of reporting requirements can sometimes degenerate into report-card driven checklist compliance at the expense of actual security improvements and investments.

As a response to this, a consortium of various organizations have collaborated to create the SANS 20CSC which is a prioritized baseline of 20 critical security controls. Members of the Consortium include the NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center, plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities.[2]

Non-Compliance Penalties

Federal agencies are required to run programs to oversee annual information security compliance reviews, the results of which are submitted to the Office of Management and Budget (OMB). Lawmakers publish annual FISMA report cards and comparative grades for the agencies.

If agencies fail to comply or receive poor scores, it could result in cuts in the agency's budget and invoke public scorn. CIOs may be called upon to testify. Contractors failing to comply can lose existing contracts and be barred from bidding on new ones.

Ineffective information security controls can result in significant risk to government operations and assets. Successful exploits can put critical operations, infrastructure, national defense, federal payments, and collections at risk. Or they cause disclosure of sensitive information, such as taxpayer data, U.S. SSN records, or intellectual property, for example.

The Barracuda Solution

The Barracuda Web Application Firewall directly addresses Critical Control 6: Application Software Security amongst others that map directly to NIST 800-53, as listed on SANS site.[3] Web Application Firewalls are recommended as "Quick Wins" to protect web applications by inspecting all traffic flowing to the web application for common web application attacks

[1]Cyber Threats and Vulnerabilities Place Federal Systems at Risk. Statement of Gregory C. Wilshusen, Director, Information Security Issues.
[2]http://www.sans.org/critical-security-controls
[3]http://www.sans.org/critical-security-controls/guidelines.php

Appendix D of Publication 800-53 (Rev. 3) catalogs eighteen security control classes for technical and program management controls. The Barracuda Web Application Firewall meets the key controls in six security control baselines, as summarized below.

Acronyms Used

RBA	Role-Based Access
AAA	Authentication Authorization and Access Control
ACL	Access Control Lists
DMZ	De-militarized Zone
ADR	Allow Deny Rules
SIEM	Security Information and Event Management
RBA	Role-Based Access
MITM	Man in the Middle attacks
MITB	Man in the Browser Attacks

Meeting FISMA (NIST 800-53) Requirements

Access Control

Ctrl. No.	Role-Based Access	Priority	
AC-3	Access Enforcement	P1	Enforces identity-based access to web applications through LDAP/AD or other AAA systems. RBA enforces role-based access to the unit. Network ACLs provide attribute-based policies for access enforcement. Strong PKI cryptography and client certificates are supported for access restrictions
AC-4	Information Flow Enforcement	P1	Acts as a boundary protection device or reverse proxy that employs rule sets to restrict information system services and information flows using packet contents, headers, domains, security attributes - filtering capability covering all the constructs from Layer 2 to Layer 7.
AC-5	Separation of Duties	P1	RBA enforces separation of duties allowing for the creation of different accounts commensurate with organizational roles. Security personnel can configure security controls without being allowed to administer audit functions.
AC-6	Least Privilege	P2	RBA module allows creation of roles with extremely granular access controls to the different modules and sub-modules of the system. Access to ports, protocols, and services in the DMZ can also be precisely administered.
AC-7	Unsuccessful Logon Attempts	P1	Blocks potential brute-force attacks by locking out clients exceeding a configurable rate of login attempts or application access.
AC-8	System Use Notification	P2	Displays a configurable system use notification message (warning banners, etc.) before granting access
AC-10	Concurrent Session Control	P1	Enforces web application session rate to protected applications to a desired maximum via session tracking.
AC-14	Permitted Actions Without Identification or Authentication	P1	Web-based Allow Deny Rules (ADRs) allow for granular specification of precise application domains that are accessible with and without authentication.
AC-17	Remote Access	P1	Enforces user access control to all the protected applications and to itself. Failed login attempts are recorded. Access logs contain authentication data for all requests to the applications.

Audit and Accountability

Ctrl. No.	Role-Based Access	Priority	
AU-3	Content of Audit Records	P1	Changes to security configuration, access to the protected applications and application attacks are all logged in comprehensive details, including timestamps, events, outcomes, source, destinations, user identity, etc.
AU-7	Audit Reduction and Report Generation	P1	Flexible report generation and scheduling provides support for near real-time audit review, analysis, and reporting requirements in AU-6 and after the fact investigations of security events.
AU-8	Time Stamps	P1	Internal system clocks are used to generate time stamps for all logs, including audit. These can synchronize with NTP servers.
AU-9	Protection of Audit Information	P2	Privileged access to all logs, including audit, is protected via RBA. Logs can be streamed out securely to external SIEM systems
AU-10	Non Repudiation	P1	Client certificates and integrated authentication and authorization mechanisms, including 2-factor, provide for non-repudiation.
AU-11	Audit Record Retention	P2	Audit records and logs are stored on persistent storage on the unit. They can be steamed out to external storage systems and this is recommended.
AU-12	Audit Generation	P1	This is facilitated by integration with external syslog and SIEM systems.
AU-14	Session Audit	P1	Captures and logs all access requests related to a user session. User sessions can be remotely viewed in real time via syslog and SIEM integration

Identification and Authentication

Ctrl. No.	Role-Based Access	Priority	
IA-2	Identification and Authentication (Organizational Users)	P1	Authentication of user identities is accomplished through the use of passwords, tokens, client certificates, and combinations thereof for multi-factor authentication. The system integrates with organizations' authentication databases such as LDAP, RADIUS, SiteMinder, etc.
IA-3	Device Identification and Authentication	P1	Network ACLs allow access control by TCP/IP addressing
IA-5	Authenticator Management	P1	Regular expression-based syntax can be used to force minimum password complexity and length. Cookies are secured by signing and encryption. PKI-based authentication validates certification paths to a trust anchor. Enforces authorized access to private keys.
IA-6	Authenticator Feedback	P1	Authentication tokens like cookies and session IDs are encrypted to prevent theft from unauthorized individuals.
IA-7	Cryptographic Module Authentication	P1	FIPS 140-2 Level-2 HSM is an option that complies with requirements. Level-1 compliance is the default configuration.

Incident Response

Ctrl. No.	Role-Based Access	Priority	
IR-4/5/6	Incident Handling, Monitoring, and Reporting	P1	SIEM integration, SNMP and email alerts, syslogs, and scheduled reporting directly facilitate the incident handling, monitoring, and reporting capabilities for security incidents.

System and Communication Protection

Ctrl. No.	Role-Based Access	Priority	
SC-3/4	Security Function Isolation, Information in Shared Resources	P1	Implements a hardened OS and networking stack that isolates all the security functions from non-security ones.
SC-5	Denial of Service Protection	P1	Acts as a boundary protection device that filters certain packets and requests (L4 and L7) to protect devices and servers on the organization's DMZ and internal network from DoS attacks. Supplemented by functions such as rate control, brute force protection, IP reputation analysis, SYN flood prevention, session tracking, etc., as well as by facilitating scaling of server farms via load balancing and application delivery functions.
SC-7	Boundary Protection	P1	Reverse Proxy deployment in the DMZ, along with VLAN support, multiple routing, and networking ensure precise communication control with the internal and external networks through explicitly managed interfaces. Rejects undefined traffic.
SC-8/9/13	Transmission Confidentiality and Integrity	P1	Supports strong PKI and cipher suite selection controls. Client certificates, CRL, OCSP provide client verification and authentication. Session IDs and cookies are signed and encrypted to prevent tampering. FIPS 140-2 Level 2 compliant models are available, while Level 1 is the default.
SC-10	Network Disconnect	P2	Proxy architecture provides complete NAC and network isolation between internal and external networks. Network assignments are dis-allocated after a period of inactivity, which is easily customized via various timeout settings.
SC-11	Trusted Path	P0	Administrator logins can be restricted to secure subnets or IP ranges via the management interface. Strong PKI can be utilized for additional authentication and verification of administrators.
SC-14	Public Access Protections	P1	Secures, speeds up, and increases the availability of publicly available web applications and services. Provides complete OWASP Top 10 protection and much more. Load balancing, content routing, caching, compression, and connection pooling keep the backend infrastructure available and responsive.
SC-18	Mobile Code	P1	Detects and blocks unauthorized, malicious mobile code (Java, JavaScript, ActiveX, etc.) from being injected into protected web applications.
SC-23	Session Authenticity	P1	Enforces session security and integrity in web applications and services by signing/encrypting session IDs and cookies. Prevents MITM, MITB, and cookie replay attacks. Protects against tampering of hidden variables.
SC-24	Fail in Known State	P1	Failover is implemented as either an active-active or a hot standby cluster. Security and configuration information is automatically synchronized securely across the cluster.
SC-26	Honeypots		Integrates in real time with Barracuda Research Labs that monitor the latest web-based malicious code and malicious sources via honeypots and other technologies/sensors.

System and Information Integrity

Ctrl. No.	Role-Based Access	Priority	
SI-2	Flaw Remediation	P1	Provides instant remediation of flaws in protected web applications for new and zero-day vulnerabilities by intercepting and blocking the attacks. Application code review, fix, and test cycle can be done in parallel without compromising security. Particularly useful where source code or expertise is not readily available.
SI-3	Malicious Code Protection	P1	Protects web accesses from all known and zero-day attacks via a layered defense approach - protocol termination, de-obfuscation, intelligent and contextual attack rule sets for whitelisting and blacklisting, limit checks, anomaly detection, cryptography. Signatures are securely updated periodically. Integrates with vulnerability scanning tools for automated patching and remediation. Regular expression-based context-sensitive rule sets minimize false positives. Policy tuner provides a single click resolution of false positives, if any.
SI-4	Information System Monitoring	P1	Monitors and relays events strategically located at the perimeter/ DMZ protecting the critical web server farms. Events are communicated over multiple channels, e.g., SIEM integration, SNMP and email alerts, syslogs, and scheduled reporting.
SI-5	Security Alerts, Advisories, and Directives	P1	Continuously complies with and addresses all the web-related security alerts and advisories in a timely manner.
SI-7	Software, Firmware, and Information Integrity	P1	Offline firmware update mechanisms are available for stronger security and integrity in a high-risk federal environment.
SI-8	Spam Protection	P1	Protects against spam, viruses, and malware when the entry and exit points are web servers. Provides file upload control and true file type detection using file contents inspection.
SI-9	Information Input Restrictions	P2	Extended matching rules can place input restrictions based on user authorization levels by analyzing the metadata in the web-based requests. Custom input types can be defined and enforced.
SI-10	Information Input Validation	P1	Screens and validates all web-based input into URL parameters and forms. Employs signature- based blacklisting as well as whitelisting to ensure conformance to valid syntax and semantics (e.g., character set, length, numerical range, acceptable values). Blocks any inputs that can be executed unintentionally inside interpreters.
SI-11/12	Error Handling	P2	Error conditions from protected servers are cloaked to ensure security through obscurity. Prevents data leakage of sensitive information like U.S. SSNs and credit card numbers. Sensitive information can be masked inside logs. Implements anti-fingerprinting techniques to stay invisible to reconnaissance activity.

About the Barracuda Web Application Firewall

The Barracuda Web Application Firewall blocks an ever-expanding list of sophisticated web-based intrusions and attacks that target applications hosted on web servers and in the cloud. The Barracuda Web Application Firewall scans all inbound web traffic to block attacks and scans all outbound traffic to provide highly effective Data Loss Prevention (DLP). It's available as a physical or virtual appliance and is deployed in front of the web application servers.

To learn more about the Barracuda Web Application Firewall, please visit http://www.barracuda.com/waf or call Barracuda Networks for a free 30-day evaluation at 1-408-342-5400 or 1-888-268-4772. For more information on our other security and productivity solutions, please visit http://www.barracuda.com/products.

About Barracuda Networks, Inc.

Protecting users, applications, and data for more than 150,000 organizations worldwide, Barracuda Networks has developed a global reputation as the go-to leader for powerful, easy-to-use, affordable IT solutions. The company's proven customer-centric business model focuses on delivering high-value, subscription-based IT solutions for security and data protection. For additional information, please visit http://www.barracuda.com.

Barracuda

© Barracuda Networks
3175 S. Winchester Boulevard
Campbell, CA 95008
United States
1-408-342-5400
1-888-268-4772 (US & Canada)
www.barracuda.com
info@barracuda.com